

**DETEKSI DAN PENCEGAHAN SERANGAN REMOTE CODE
EXECUTION TERHADAP WING FTP WEB SERVER
MENGUNAKAN SNORT**



SKRIPSI

Disusun sebagai salah satu syarat menyelesaikan Jenjang Strata I
pada Program Studi Informatika Fakultas Komunikasi dan Informatika
Universitas Muhammadiyah Surakarta

Oleh:

MUHAMMAD TRIWIBOWO

NIM : L200110114

**PROGRAM STUDI INFORMATIKA
FAKULTAS KOMUNIKASI DAN INFORMATIKA
UNIVERSITAS MUHAMMADIYAH SURAKARTA
2015**

HALAMAN PERSETUJUAN

Skripsi dengan judul

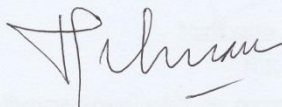
**DETEKSI DAN PENCEGAHAN SERANGAN REMOTE CODE
EXECUTION TERHADAP WING FTP WEB SERVER
MENGUNAKAN SNORT**

telah di periksa, disetujui untuk diajukan dalam sidang pendadaran pada :

Hari : Senin

Tanggal : 1 Juli 2015

Pembimbing

Helman Muhammad, S.T., M.T.

NIK: 077 1394

HALAMAN PENGESAHAN

**DETEKSI DAN PENCEGAHAN SERANGAN REMOTE CODE
EXECUTION TERHADAP WING FTP WEB SERVER
MENGUNAKAN SNORT**

dipersiapkan dan disusun oleh

Muhammad Triwibowo

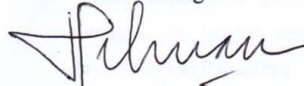
NIM : L200110114

telah dipertahankan di depan Dewan Penguji

pada tanggal 4 Juli 2015

Susunan Dewan Penguji

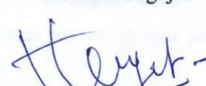
Pembimbing



Helman Muhammad, S.T., M.T.

NIK : 0771397

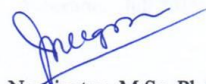
Dewan Penguji I



Hernawan Sulistyanto, ST., M.T

NIK : 082

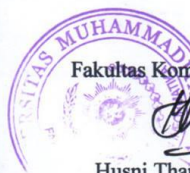
Dewan Penguji II



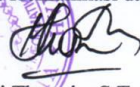
Nurgiyatna, M.Sc., Ph.D

NIK : 881

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar sarjana jenjang strata I pada program studi Informatika
Tanggal 9 Juli 2015.



Dekan
Fakultas Komunikasi dan Informatika



Husni Thamrin, S.T, MT., Ph.D.

NIK : 706



Ketua Program Studi
Informatika



Dr. Heru Supriyono, M.Sc

NIK : 970

KONTRIBUSI

Dengan ini saya menyatakan bahwa skripsi ini belum ada karya yang sama yang telah diajukan sebelumnya untuk memperoleh gelar kesarjanaan di Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Berikut saya sampaikan daftar kontribusi dalam penyusunan skripsi:

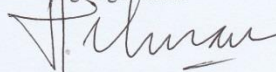
1. Penulis membangun sistem keamanan jaringan komputer ini dengan beberapa referensi baik dari buku, skripsi, jurnal, ebook, maupun internet.
2. Tahap instalasi beberapa *software* baik pada komputer client maupun komputer *server*, konfigurasi snort dan *firewall*, dilakukan sendiri oleh penulis dengan mengikuti panduan referensi yang telah disebutkan dalam daftar pustaka laporan skripsi ini.
3. Persiapan peralatan penelitian, tahap deteksi serangan, tahap pencegahan serangan, dan langkah pengujian snort dilakukan penulis dengan dibantu oleh Bryan Pingkan Ramadhan
4. Penulisan laporan skripsi ini dilakukan oleh penulis sendiri.

Demikian pernyataan dan daftar kontribusi ini saya buat dengan sejujurnya. Saya bertanggungjawab atas isi dan kebenaran daftar di atas.

Surakarta, Juli 2015

Mengetahui

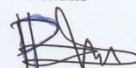
Pembimbing Tugas Akhir



Helman Muhammad, S.T., M.T.

NIK : 0771397

Penulis



Muhammad Triwibowo

MOTTO DAN PERSEMBAHAN

MOTTO

Tidak sepatutnya bagi mukminin itu pergi semuanya (ke medan perang). Mengapa tidak pergi dari tiap-tiap golongan di antara mereka beberapa orang untuk memperdalam pengetahuan mereka tentang agama dan untuk memberi peringatan kepada kaumnya apabila mereka telah kembali kepadanya, supaya mereka itu dapat menjaga dirinya.

(Q.S At- Taubah :122)

Tak ada rahasia untuk menggapai sukses.

Sukses itu dapat terjadi karena persiapan, kerja keras, dan mau

Belajar dari kegagalan

Gen. Collin Powell

*Sesuatu akan terasa indah apabila
di lakukan dengan rasa ikhlas dan sabar*

(Penulis)

PERSEMBAHAN

Sebagai rasa syukur penulis persembahkan karya ini kepada :

1. Allah SWT yang selalu melimpahkan rahmat dan hidayah bagi hambaNya serta yang selalu menunjuki ke jalan yang lurus.
2. Kedua orang tuaku tercinta, Almarhum Bapak Imlak dan Ibu Muryani yang telah membimbing saya dari kecil hingga sekarang ini, untuk setiap nasihat dan doa yang dipanjatkan untuk kesuksesan penulis, serta dukungan moril dan materiilnya.
3. Kepada kakak saya Siti Muslimah dan Muhammad Yulianto yang telah memberikan nasihat, semangat dan motivasi.
4. Kepada bulikku Umi Nurjanah yang selalu memberikan motivasi dan nasihat.
5. Kepada keluarga besar saya yang ada di Solo.
6. Kepada teman saya Athika Ratma Sari yang telah memberikan motivasi selama ini.
7. Kepada semua teman saya di grub IDM yang sangat gokil yang telah memberikan semangat kepada saya yaitu Aan, Fuad, Luthfi, Vopy, devanda, Taid, Bayu, Doni, Nega, Erlis, Herlambang, dan masih banyak yang lain.
8. Kepada semua teman saya yang baik hati Theo, Yudhi, Bahrudin, Dedy, Arifin, Bahsid, Didik yang memberikan semangat.
9. Almamater

KATA PENGANTAR



Alhamdulillah rabbil'alamini atas segala nikmat iman, Islam, kesempatan, serta kekuatan yang telah diberikan Allah Subhanahuwata'ala sehingga Penulis dapat menyelesaikan skripsi ini. Shalawat beriring salam untuk tuntunan dan suri tauladan Rasulullah Shallallahu'alaihiwasallam beserta keluarga dan sahabat beliau yang senantiasa menjunjung tinggi nilai-nilai Islam yang sampai saat ini dapat dinikmati oleh seluruh manusia di penjuru dunia.

Skripsi ini dibuat sebagai salah satu syarat untuk mendapat gelar sarjana komputer dari Program Studi Teknik Informatika Universitas. Mempersembahkan ucapan terima kasih dan penghargaan setinggi-tingginya dengan segala kerendahan hati, kepada:

1. Allah Subhanahu Wata'ala yang maha segalanya.
2. Bapak Helman Muhammad, S.T., M.T. selaku Pembimbing yang telah berkenan untuk meluangkan waktu dan membimbing serta mengarahkan penulis sehingga terselesaikannya penyusunan skripsi ini.
3. Kedua orang tuaku tercinta, Almarhum Bapak Imlak dan Ibu Muryani.

Akhirnya, dengan segala kerendahan hati penulis menyadari masih banyak terdapat kekurangan-kekurangan, Semoga skripsi ini bermanfaat bagi semua yang membacanya amin.

Surakarta, Juli 2015

Penulis

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PERSETUJUAN	ii
HALAMAN PENGESAHAN	iii
DAFTAR KONTRIBUSI	iv
PERSEMBAHAN DAN MOTTO	v
KATA PENGANTAR	vii
DAFTAR ISI	viii
DAFTAR BAGAN	xi
DAFTAR GAMBAR	xii
DAFTAR LAMPIRAN.....	xiv
ABSTRAK.....	xv
BAB I PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah.....	2
1.4 Tujuan Penelitian.....	3
1.5 Manfaat Penelitian	3
1.6 Sistematika Penulisan	4
BAB II TINJAUAN PUSTAKA.....	5
2.1 Telaah Pustaka.....	5
2.2 Landasan Teori	11
2.2.1 Keamanan Jaringan Komputer	11
2.2.2 Intrusion Detection System	12

2.2.3	Intrusion Prevention System.....	15
2.2.4	Snort.....	17
2.2.5	Metasploit Framework	20
2.2.6	Wing FTP Web Server	22
2.2.7	Remote Code Execution	24
2.2.8	Firewall.....	25
BAB III	METODOLOGI PENELITIAN.....	26
3.1	Alokasi Waktu Penelitian	26
3.2	Perangkat yang Dibutuhkan.....	26
3.2.1	Komputer Server.....	26
3.2.1.1	Perangkat Keras	26
3.2.1.2	Perangkat Lunak	27
3.2.2	Komputer Client	27
3.2.2.1	Perangkat Keras	27
3.2.2.2	Perangkat Lunak	27
3.3	Metode Penelitian	27
3.4	Alur Penelitian	28
3.5	Perancangan Sistem	30
3.5.1	Konfigurasi Rule Snort.....	32
3.5.2	Konfigurasi Firewall.....	37
3.5.3	Pengujian Sistem	43
BAB IV	HASIL DAN PEMBAHASAN	44
4.1	Hasil Penelitian.....	44
4.1.1	Pengujian Sistem Tahap Deteksi Serangan	44
4.1.2	Pengujian Sistem Pencegahan Serangan	51

4.2	Pembahasan	55
BAB V	PENUTUP	57
5.1	Kesimpulan	57
5.2	Saran	58
	DAFTAR PUSTAKA	59
	LAMPIRAN	

DAFTAR BAGAN

3.1	Diagram Alir Alur Penelitian	28
3.2	Diagram Alir Perancangn Sistem.....	31
4.1	Diagram Alir Pencegahan	52

DAFTAR GAMBAR

2.1	Komponen IDS	20
2.2	Contoh Script Remote Command Execution	24
3.1	Tampilan konfigurasi firewall	38
3.2	Tampilan Advanced Setting	38
3.3	Tampilan Inbound rule	39
3.4	Tampilan konfigurasi rule	39
3.5	Tampilan program konfigurasi firewall	40
3.6	Tampilan protocol dan port	40
3.7	Tampilan tahap scope	41
3.8	Tampilan tahap action	41
3.9	Tampilan tahap profil	42
3.10	Tampilan pengisian tahap serangan	42
3.11	Tampilan firewall yang sudah selesai di setting	43
4.1	Tampilan folder metasploit	46
4.2	Tampilan metasploit console	46
4.3	Tampilan mencari serangan wing ftp server	47
4.4	Tampilan melakukan exploit wing ftp server	47
4.5	Tampilan melihat target exploit	48
4.6	Tampilan port username dan password	48
4.7	Tampilan menjalankan exsploit	49
4.8	Tampilan serangan masuk ke target	49
4.9	Tampilan file txt sbml dihapus	50
4.10	Tampilan file txt yang sudah dihapus	50

4.11 Tampilan peringatan serangan Remote Code Execution	51
4.12 Tampilan firewall mencegah RCE.....	54
4.13 Tampilan metasploit gagal menyerang target	54

DAFTAR LAMPIRAN

A. Instalasi Metasploit Framework.....	63
B. Lampiran 2 Instalasi Kiwi Log Viewer.....	66
C. Lampiran 3 Instalasi Wing FTP Server.....	68
D. Lampiran 4 Instalasi Snort	74

ABSTRAK

Masalah keamanan sebuah jaringan amat sangat rentan terhadap serangan dari berbagai pihak. Alasan dari serangan tersebut tentu saja beragam. Diantaranya yaitu alasan untuk merusak, balas dendam, politik, atau Cuma iseng – iseng saja untuk unjuk kemampuan. Di balik kemudahan pengaksesan informasi yang disediakan oleh internet terdapat bahaya besar yang mengintai, yaitu berbagai macam serangan yang berusaha mencari celah dari sistem keamanan jaringan komputer yang digunakan. Serangan-serangan itu dapat mengakibatkan kerusakan data dan bahkan kerusakan pada *hardware*.

Penelitian ini akan mengidentifikasi bagaimana suatu *serangan Remote Code Execution* bekerja terhadap *Wing File Transfer Protokol (Wing FTP Web Server)*, dan kemudian melakukan pendeteksian serangan menggunakan *snort*. Deteksi dan pencegahan dilakukan dengan rancangan membuat *firewall* aktif untuk mengidentifikasi setiap data yang masuk kedalam *server*, apakah data tersebut merupakan serangan *Remote Code Execution* atau bukan.

Hasil dari penelitian ini adalah suatu sistem keamanan jaringan yang mampu mendeteksi dan mencegah terjadinya serangan *Remote Code Execution* terhadap *Wing FTP Web Server*. Sistem yang dihasilkan dalam penelitian ini bisa dilihat melalui pengujian terhadap sistem, dalam hal ini mencakup 2 tahap, yaitu tahap deteksi serangan dan tahap pencegahan serangan.

Kata kunci : Keamanan Jaringan Komputer, *Remote Code Execution*, IDS *Snort*, *Kiwi Log Viewer*, *Metasploit Framework*, *Firewall*